ENCLOSURE (B)

SELF ASSESSMENT GUIDELINES

June 1998

DOE HEADQUARTERS
ADP SECURITY SELF ASSESSMENT GUIDELINES
FOR SENSITIVE UNCLASSIFIED SYSTEMS

DATE OF REVIEW ____/____/____

ORGANIZATION:_____ LOCATION:_____ ROOM # _____

ACPPM:_____ REVIEWER:_____
(Printed Name) (Printed Name)

The following generic checklist is provided to assist ACPPMs in evaluating conformance with the DOE Headquarters Unclassified Computer Security Program. While this list is not comprehensive, it will enable users to identify strengths, weaknesses, and areas of concern within their individual programs.

GENERAL OVERALL PROGRAM

1. How many systems are under your responsibility? Standalone_____ Network_____

2. Which, if any, sensitive major applications does your organization control?_____
_____

	Yes	No	
3.	___	___	Is the ACPPM appointment letter up to date?
4.	___	___	Have general support systems/major applications been identified and covered by a CSPP?
5.	___	___	Have applications processing sensitive information been identified/included in host CSPPs?
6.	___	___	Does the organization have a program in effect to address Public Law 99-474, Computer Fraud and Abuse Act of 1986, and requirements of 10 CFR 1010.207, Use of Government Property?.
7.	___	___	Does the organization have a copyright protection enforcement program?
8.	___	___	Have all personnel having computer security responsibility received training?
9.	___	___	Do contractors maintaining, supporting, or accessing federal systems receive computer security training?
10.	___	___	Do all personnel who operate, control access, or design, develop, install, modify, service, or maintain the security features on sensitive systems have DOE approval and need-to-know for access to that information?
11.	___	___	Are persons who are not approved for viewing sensitive information escorted when access to the system is necessary?
12.	___	___	Is the general support system(s) hardware in a government or contractor protected area, i.e., DOE facilities or in protected contractor offices?
13.	___	___	Does the ACPPM have a list of (1) persons authorized physical access to their sensitive systems; (2) persons authorized to lock, occupy, and unlock the facility; (3) persons to be notified in an emergency?

	Yes	No	
14.	___	___	Are all storage media (backup tapes, diskettes, etc.) associated with general support systems and major applications properly marked and protected commensurate with the sensitivity of the information for which the system processes?
15.	___	___	Are the Headquarters CPP and a DOE MA-427 "Computer Security Guide for Users" accessible to each user?
16.	___	___	Are all security relevant hardware and software modifications tested; are results reviewed by the ACPPM; and is the security certification updated?
17.	___	___	Does the organization have a periodic security awareness program for all users?
18.	___	___	Are all users aware of sensitive document media marking and labeling procedures and is there evidence of compliance?
19.	___	___	Are all users aware of and comply with DOE Headquarters sensitive material destruction procedures?
20.	___	___	Are checks conducted for official use of Government property and is documentation on file with the ACPPM?
21.	___	___	Are users aware of their responsibility for reporting security incidents?
22.	___	___	Are system resident files adequately backed up and stored away from the processor area?

NETWORKED SYSTEMS

	Yes	No	
23.	___	___	Is host system documentation available for review? Documentation should consist of the current approved Computer Security and Privacy Plan (CSPP), system security certification(s) and system approval(s).
24.			Are documents containing the following information available for review?
	___	___	(a) System Inventory
	___	___	(b) System Configuration Diagrams
	___	___	(c) Hardware and Software Change Control Procedures
	___	___	(d) Security Administration Procedures
	___	___	(e) System Operating Procedures
	___	___	(f) System Shut-down Procedures
	___	___	(g) Media Destruction Procedures
	___	___	(h) Computer Security Training/Awareness Records to support training program implementation
	___	___	(i) Risk Assessment Results

	Yes	No	
	___	___	(j) Contingency Plan
25.	___	___	Is the host processor physically protected?
26.	___	___	Is the host processor protected from power failures by an uninterruptible power supply?
27.	___	___	Is an equal level of protection enforced on all computing environments that have simultaneous connections to the system (system high concept)?
28.	___	___	Are users required to enter a unique USERID and password to gain access to the system(s)?
29.	___	___	Are passwords at least 6 characters in length?
30.	___	___	Are appropriate logon features (e.g., nonconcurrent logon, accessible hours) implemented?
31.	___	___	Do users receive a system message each time they logon the network documenting the date, time, location, and number of unsuccessful logon attempts since their last session or date and time of last successful logon?
32.	___	___	Are security software features implemented that suspend a users ability to access the system after a specified number of unsuccessful logon attempts?
33.	___	___	Does the ACPPM/System Administrator maintain a record, to include, source of all software on the system?
34.	___	___	Are the levels of user privileges and are criteria for granting those privileges documented?
	___	___	(a) Do some users have special or global access privilege?
			If yes, how many people?_____
	___	___	(b) Does the System Administrator maintain a list of these people?
35.	___	___	Is user need-to-know enforced by the security software?
			(a) Operating system?
			(b) Application software?
			(c) Special security software?
36.	___	___	Is the System Administrator's password written down, marked sensitive and stored in a sealed envelope in a security container where it may be accessed by a designated individual in the event of an emergency?
37.	___	___	Does the System Administrator have a backup in the event they are unavailable during an emergency?
38.	___	___	Are users forced to change their password periodically?
39.	___	___	Is the procedure for granting authorization to access the system documented, and is it adequate?

	Yes	No	
40.	___	___	Is there evidence that the ACPPM, or an agent of the ACPPM, reviews system audit reports on a scheduled basis?
41.	___	___	Is there a Continuity of Operations Plan (COOP) for mission-essential applications and systems?
42.	___	___	Are system resident files adequately backed up and are the backups tapes stored away from the system?
43.	___	___	Does the system protect files and allow access to specific files as designated?
44.	___	___	Are automated file access control lists only accessible to authorized users?
45.	___	___	Are user privileges and access controls verified as part of the process to create a new user?
46.	___	___	Are accounts reviewed for activity (how long without access)? Are inactive accounts disabled or deleted?
47.	___	___	Does the system utilize a monitor or processor time-out feature?
48.	___	___	Is there evidence that an effective procedure is in effect which attempts to ensure that users who no longer require access to the system are deleted from access?

REMARKS: